Remarks

Claims 23, 24, 26-35, and 40-51 are pending in the application. Claims 23, 24, 26-35, and 40-51 are rejected. Claims 26 and 40 are amended herein. No new matter is added. All rejections are respectfully traversed.

Claims 26 and 40 are amended to correct a minor typographical error.

In a network that requires each host device to have firewall capability in its network interface device, e.g., NIC card, the invention allows a host device having a network interface without a firewall to connect to the network. The host device must have a hardware firewall attached. The invention routes data transferred from the network, through the network interface, to the attached firewall for processing before the host receives the data. Before the network connection is allowed, a configuration integrity check of a software component on a host device is performed and the check must pass.

Claims 23, 26-30, 32, 33, 40, 41, 43-46, 48 and 49 are rejected under 35 U.S.C. 102(e) as being anticipated by Villa, et al., (U.S. 6,550,012 – "Villa").

Villa describes an active firewall. According to Villa, components that detect and decide whether or not to act on specified events in a network can participate in authenticated and encrypted communications. The components engaged in the communications can be sensors, arbiters and actors, e.g., a firewall. The components use cryptographic keys, digital certificates and digital signatures to engage in the authenticated and encrypted

communications. The Examiner's use of the Villa reference is perplexing to the Applicants, because it really has nothing to do with what is claimed. There is no description of a network that requires each host device to have firewall capability in its network interface device, or a method that allows a host device having a network interface without a firewall to connect to the network.

For instance, claimed is allowing a connection to said network to be established when said host device uses said network interface device without the required firewall capability only if a firewall device comprising a hardware implemented firewall is coupled to said host device. So, instead of the host device using a network interface device having a firewall capability as required by the network, the invention allows a host device having a network interface device without firewall capability to connect to said network if the host device instead has a hardware implemented firewall coupled to it. Col. 8, lines 38-55, cited by the Examiner, is completely devoid of any teaching of what is claimed, see below:

> 1. Eliminating Human-to-human Communication
>
> An important design consideration in the creation of an active firewall of the present invention is the replacement of communication between humans with software-based communication. Consider, for instance, the following typical practice today. Suppose an IT worker running a scanner program discovers a vulnerability on a company network. If that individual does not have appropriate access level (i.e., system privileges) to make modifications for correcting the situation (as is often the case), he or she will have to inform the appropriate member of the IT team who is capable of making the appropriate changes. In this act of human-to-human communication, it is taken for granted that the communication is secure—that is, that there is no unauthorized participant or listener. In other words, the communication occurs in a manner such that "spoofing" is not possible. Thus, in this example, the IT worker achieves secure, authenticated communication by telling someone that he or she personally knows and trusts.

The cited section describes human-to-human communication between IT personnel and individual users who are apparently on friendly terms, in that they personally know and trust each other. While teaching personal trust between people is nice, it has absolutely nothing to do with what is claimed. The Examiner is requested to point out, with specificity, exactly which words, above, mean a firewall capability in said communication interface device that is required by the network for data transfer between the network and a host device, or allowing a connection to said network to be established when said host device uses said network interface device without the required firewall capability, or allowing a connection only if a firewall device comprising a hardware implemented firewall is coupled to said host device, as claimed.

It should now be understood that Villa can never anticipate what is claimed. MPEP 2131 explicitly states that in order to anticipate a claim "each and every element as set forth in the claims" must be found in the prior art reference. "The identical invention must be shown in as complete detail as is contained in the ... claim." The Examiner's rejection ignores at least the explicit limitations recited in independent claim 26 that recite a hardware implemented firewall coupled to a host device, a host device having a network interface device without firewall capability as required by the network being allowed to connect to the network only if a hardware implemented firewall coupled to a host device, or any such requirement in a network. There is no teaching or suggestion in Villa to allow access to a network in the novel manner recited in the claims.

The remaining elements of independent claim 26 recite receiving data from said network over said connection establish via said communication interface device, processing said data with said hardware implemented firewall, transferring said processed data to said host device, and performing a configuration integrity check of a software component on a host device, wherein said configuration integrity check is performed before said network connection is allowed, wherein said connection is allowed only if said configuration integrity check passes.

For the above remaining elements of claim 26, the Examiner inexplicably refers to col. 14, lines 15-32, below:

> During system operation, the Active Security Layer **350** (employing the PGPsdk™ run-time library) provides socket communication, establishment of communication sessions, exchanging of authentication certificates, and the like. At the time of secure communication, participating components may exchange respective digital certificates, each examining the certificate of the other for determining whether it has been signed by a party that is trusted. Here, the PKI has served as the provider of certificates. In the event that the certificates of respective components are trusted by the same party (i.e., PKI **360**, as configured by the system administrator), the components may now trust one another. Thus after successfully exchanging certificates (i.e., accepted as being trusted), communications between the components may proceed in a secure manner. Since the root of trust occurs at the PKI **360**, access to configuration of the PKI **360** itself for requesting/issuing certificates should be restricted (e.g., system administrator-level privileges).

Again, the Examiner is requested to specifically explain which words above mean receiving data via a network interface device that doesn't have firewall capability, but is used by a host device with a hardware implemented firewall coupled to it. There is no teaching of processing said data with said hardware implemented firewall, or transferring said processed data to said host device that the hardware implemented firewall is coupled to. Nor is there any teaching of anything resembling a configuration ***integrity*** check. A

person of ordinary skill in the art would never confuse setting up authenticated communication with checking the integrity of a configuration of a software component on the host device, as claimed. Apparently, Villa fails to teach a single element of what is claimed. Therefore, the rejection should be reconsidered and withdrawn. Claim 40 is substantially similar to claim 26, with the exception of the configuration integrity check performs a hash on said software component to produce a hash value and comparing said hash value with a stored hash value, which is also not taught in Villa. The Examiner has cited the identical sections of Villa for claims 26 and 40. Therefore, the arguments above are asserted for claim 40 as well. The rejection of claim 40 should be withdrawn for the same reasons as set forth above.

Claims 23 and 41 recite the host device routing said data to said firewall device to be processed by said hardware implemented firewall, said routing taking place at a physical layer in said data stack. As stated above, col. 8, lines 38-55, cited by the Examiner, is completely devoid of any teaching of what is claimed. There is nothing in the section that even remotely resembles what is claimed.

In claim 27, as in claim 40, the configuration integrity check is performed by performing a hash on said software component to produce a hash value and comparing said hash value with a stored hash value. The cited section of Villa describes digital certificate validation and cryptographic hashing, see col. 15, lines 43-54, below:

If each respective component is able to successfully validate the certificate received from the other, secure communication ensues. From that point on, communication occurs in a secure, authenticated manner, with each message or blob being digitally signed or fingerprinted, for instance, using a cryptographic hash or message digest. This is indicated by step **517**. Any alteration to the message breaks the digital fingerprint and, therefore, may easily be detected. If desired, encryption may also be (optionally) applied to the communication messages. In those embodiments intended for export from the United States, however, encryption may be limited (e.g., as to key length) or removed.

Cryptographic hashing of communications can never anticipate performing software configuration integrity checking by hashing, as claimed. The same is true for claims 28 and 44, where said stored hash value resides on said firewall device; for claims 29 and 45 which recite sending an alert if said configuration integrity check fails; and for claims 30 and 46 which recite storing an alert if said configuration integrity check fails.

Claims 32 and 48 recite transferring data to be transferred over said network by said communication interface device to said firewall device; and processing said data with said hardware implemented firewall, wherein said data is processed by said hardware implemented firewall before it is transferred over said network connection established via said communication interface device. In claims 33 and 49, the host device routes said data to said firewall device before it is sent to said communication interface device, said routing taking place at a physical layer in said data stack. Again the Examiner refers to col. 8, lines 38-55. As stated above, the cited section can never anticipate what is claimed. The Examiner is requested to provided a detailed explanation of his reasoning for citing col. 8, lines 38-55, because the relevance of the section is simply not understood.

In claim 43, as in claim 26, the configuration integrity check is performed before said network connection is allowed and wherein said connection is allowed only if said configuration integrity check passes. Villa never teaches a configuration integrity check of a software component on a host device, as claimed. Villa is entirely useless for teaching any element of what is claimed.

Claims 24, 34, 35, 42, 50 and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Villa in view of Mayer (U.S. 7,003,562).

As stated above with respect to claims 23, 26-30, 32, 33, 40, 41, 43-46, 48 and 49, Villa fails to teach a single element of what is claimed. Mayer fails to cure the defect of Villa. Mayer compares actual network configuration against a corporate network configuration policy to identify violations of the corporate policy. Mayer is useless for making the invention obvious.

Claims 24 and 42 recite sending policies to said firewall device, wherein the operation of said hardware implemented firewall is modified. Mayer, at col. 4, lines 5-44 describes an analysis platform determining devices in a network that are relevant to a network policy to construct a network configuration model, which it compares to the network policy to identify and record violations of the network policy. Claimed is sending policies to said firewall device, wherein the operation of said hardware implemented firewall is modified. Mayer is irrelevant to what is claimed.

Claims 34 and 50 recite performing a configuration integrity check of a software component on said host device; and sending policies to said

firewall device, wherein the operation of said hardware implemented firewall is modified. As stated above with respect to claim 26, encrypted communications have nothing to do with a configuration integrity check of software. The rejection should be reconsidered and withdrawn. The same is true for claims 35 and 51, which recite sending an alert if said configuration integrity check fails.

Claims 31 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Villa in view of Hallinan, et al. (U.S. 6,996,614 – "Hallinan").

Claims 31 and 47 recite swapping resource spaces in said host device that are reserved for said communication interface device and said firewall device, wherein said host device treats said communication interface device as said firewall device and vice versa; and said communication interface device transferring data received from said network to said firewall device, wherein said firewall device processes said data with said hardware implemented firewall.

As stated above with respect to claims 23, 26-30, 32, 33, 40, 41, 43-46, 48 and 49, Villa fails to teach a single element of what is claimed. Hallinan fails to cure the defects of Villa.

Hallinan describes a method for allocation the resources of a service provider to a plurality of users. Hallinan is very far a field from the purpose of the invention. There is no motivation provided in Hallinan or Villa to combine the references. Even if there were, which is not admitted, the

combination of Villa and Hallinan falls miserably short of teaching what is claimed. Hallinan describes allocating first and second resources of a queue manager to applications and using the same interface between an application and the resource dispenser as is used between the resource dispenser and the queue manager. Hallinan does not describe swapping resource spaces, as the Examiner asserts, but using a single interface between applications, a resource dispenser and a queue manager. Therefore, Hallinan can never be used to make the invention obvious.

It is believed that this application is now in condition for allowance. A notice to this effect is respectfully requested. Should further questions arise concerning this application, the Examiner is invited to call Applicant's attorney at the number listed below. Please charge any shortage in fees due in connection with the filing of this paper to Deposit Account 50-3650.

Respectfully submitted,
3Com Corporation,

By _____

Andrew J. Curtin
Attorney for the Assignee
Reg. No. 48,485

350 Campus Drive
Marlborough, MA 01752
Telephone: (508) 323-1330
Customer No. 56436